Communication, Control, and Security Functional Working Group (CCSFWG) 31 March - 2 April 1997 Meeting Minutes

1. Introduction. The Communication, Control, and Security Functional Working Group (CCSFWG) Chairman, Mr. Lebbeus Curtis of the Joint Interoperability and Engineering Organization (JIEO)/JEKH convened the CCSFWG meeting on 31 March 1997 at 0900 hours. The meeting was held at the Logicon facility in Reston, Virginia.

2. Opening Remarks. Mr. Curtis welcomed all attendees to the meeting. The meeting attendees introduced themselves. The CCSFWG Charter was sent out electronically to the CCSFWG membership and comments were received from Mr. Harry Featherstone of the Logistics Management Institute and Mr. Tom Wheel. Their comments have been incorporated and the revised charter will be discussed. A revised Part 10 was distributed to the CCSFWG membership and posted in the Commerce Business Daily (CBD). Comments that have been received were incorporated by Mr. Mike Schulze of Logicon and will be discussed. The 997 and 242 will also be discussed. Mr. Manny Vlastakis of JIEO/Center For Standards and Mr. Nat Obey of Logicon will discuss security issues. Tuesday will be an open forum with the Value Added Network (VAN) providers and software vendors. Lieutenant Colonel Mike McFarren or his representative will discuss the status of the Electronic Commerce Processing Node (ECPN) software and the implementation schedule for incorporating Part 10 features.

The group approved the agenda as proposed.

3. CCSFWG Charter.. Editorial changes were made. Section 4, Roles and Responsibilities, was changed to reflect that the chair of CCSFWG is the official DoD representative at X12C.

Section 5, Guidelines and Operating Procedures, the first paragraph was changed in the area of selecting the Chair and Vice Chair: "... will be selected by the Functional Working Group through a nomination process, followed by a vote by the members present ..." rather than by voice vote. The second paragraph was changed as follows: "... Appeals to membership determinations by the Functional Working Group will be forwarded to the Chairs of the FESMCC and DoD EDISMC, as applicable, for resolution. Member agencies and components shall designate, in writing to the Chair, a principal representative and alternate for voting purposes ..." An e-mail will be sent out by the Chair to the CCSFWG membership requesting that the voting reps and alternates be identified. Paragraph 3 was changed as follows:"Electronic voting will be conducted to ensure any recommendations or proposals deliberated on at a session are fully staffed through all appropriate avenues." Paragraph 4 was changed for negative electronic votes in that they "... will be considered by the Chair provided they

include specific technical or operational considerations why the proposal or recommendation should not be accepted." The normal voting period will be 15 day and urgent will be 7 days. Paragraph 5 was changed to allow for situations where either Federal Civilian or DoD activities feel that a single vote per component approach will not provide clear resolution regarding the issue at hand, "... the Chair may initiate a two-stage voting process, with all the DoD Services and Agencies voting first to determine the DoD position which will be considered the DoD vote in a second vote by all Federal Civilian Agencies (thereby replicating the voting process of the FESMCC)." The updated charter will be provided electronically for review. After approval by the CCSFWG membership, the revised charter went be sent to the EDISMC and FESMCC for approval.

4. Changes to Part 10. Mr. Mike Schulze, Logicon, discussed that revised Part 10. Comments from the CBD review include: allowing both digital signature and encryption at the GS and TS levels; changes in the GS08 schema; requesting a DUNs number to be placed in the ISA field for public transactions rather than "ZZ" and the string 'PUBLIC' as an address; add more codes to 1570 in the SVA segment. Two sets of comments received from Mr. Featherstone and Mr. Bob Miller, GE, have not be incorporated but included in the text to be resolved by the group.

The group discussed the comments to Part 10 and a revised document will accompany the minutes. Some of the major issues discussed included: transmission and receipt of ASCII data within the ECI; Base 64 filtering of binary segments; a definition of ECI; Changes to the GS08 schema; Padding or filling fields with blanks and space characters

5. Changes to TS 242. Mr. Schulze facilitated this discussion. The group discussed the comments to TS 242. Changes were made to the introduction; DE 353 Transaction Set Purpose Code; DE 337 Time; Hierarchial Level (HL) segment; Interchange Identification segment (IIS)/HL loop; Name segment/HL loop; Quantity segment/STS loop. A revised document will accompany the minutes.

6. Security Briefing. Mr. Nat Obey, Logicon, presented this briefing. He addressed the status of current projects, planned projects, and key security issues. A survey has been e-mailed to the EC/EDI federal and civilian functional users to gather security requirements.

7. Part 10 Update (Open forum). Mr. Mike Schulze, Logicon facilitated this discussion. The following issues were discussed:

- Base 64 filtering. The filtering of binary data will cause a 6-33% increase in file size.

Many of the participants felt that the filtering of binary data should be

left to the two trading partners. The group agreed to change the text as follows: "The Federal Government Electronic Commerce Infrastructure (ECI) shall send and receive textual data ASCII encoded. If unencrypted binary segments are filtered, Base 64 filtering shall be used."

- GS/GE control numbers. It was brought out that uniqueness is achieved by four elements instead of three. "The Group Control Number value (GS06), together with the Application Sender's Code (GS02), Receiver's codes (GS03), and the Functional Group ID (GS01) ..."

- ISA Naming Schemes. There is a problem with File Name routing. It was stated that the ECPN plans to route on the DUNs number. There are plans to establish DUNs numbers for ECPNs and Publics.

● The following implementation note will be added to clarify addressing issues for public transactions. " 4. In the ECI, when an interchange contains public transactions, the ISA08 will be addressed individually to all certified VANs, not each IPoT. The ISA06 will contain the ECPNs address."

● The following implementation note will be added to the VLA: "Within an interchange, all GS02/GS03 code pairs shall be identical throughout the interchange. In the case of a public transaction, an additional limitation shall allow for only one transaction set per group, one group per interchange."

● Additional implementation notes will be added to describe what the Government expects and when as it relates to TA3s. The TA3 reason codes will be revisited for applicability.

● An implementation note will be added to the section on 997 to define syntactical correctness of an IC.

8. Part 10 Security Update (Open forum). Mr. Schulze facilitated this discussion. The group considered the following:

a. If the 4010 security segments of X12.58 are implemented, they do not provide a solution for transaction prior to 4010.

b. A separate meeting should be convened to discuss security issues. This implies deleting or significantly modifying the security section of Part 10.

c. Provide a few paragraphs that will explain some of the issue discussed.

d. Implement the 4010 version of the S1 and S2 security segment using a post/pre- processor function.

e. Implement security at a lower level (socket, session, etc.) between the ECPN and the VANs.

The group decided to modify section 10.5 and convene a meeting at a later date to
discuss security issues. It was requested that the results of the security requirements survey be documented and presented at the security meeting. Mr. Dan Codman was asked to prepare a strawman of a requirements matrix. The major issues discussed included:

- Security segments. The 3070 version of the X12.58 security segments contained in this document are in the process of being changed. The balloted version of X12.58 deletes the S1 and S2 segments and replaces them with the S3 and S4 segments. Radical changes in the structure and placement of the assurance segments were also made. The new segments will be available in version 3072. The Government has a standing policy which does not allow the implementation of subreleases of X12 which means the new segments will not be available for use in the ECI until version 4010. Version 4010 is scheduled to be available in January 1998. The group decided that since security features would not be implemented in the ECI until October and version 4010 would be available in January, it would be impractical to implement the 3070 security segments and then replace them a few months later with 4010.

The 3070 S1 and S2 security segments cannot provide security for transaction sets 3060 or early (e.g., 2003). The majority of the ECI implementations of X12 are prior to 3070. The group decided that it is futile to implement the 3070 S1 and S2 segments for so few transactions.

It was suggested that the 3070 X12.58 security segments could be applied to a transaction by a preprocessor function (before translation) for transaction sets 3060 and earlier. The software vendors felt that any errors that occurred in the preprocessor could not be reported in an X12 format.

- Security implementation. Part 10 features will be implemented in the ECI in a phased approach. The earliest security can be implemented will be October. It was noted the Government does not have a validated set of security requirements. The EC/EDI functional users will be surveyed to gather these requirements. It was requested that the VANs also provide their security requirements.

End-to-end security is not feasible if EDI translation occurs at an intermediate system. The current infrastructure will not provide security between AIS and the translation point or the VAN and the TP. Part 10 implements translator to translator security.

Implementation of a secure socket layer was discussed. It was brought out that a secure socket layer may be implemented between the AIS/GPoT and IPoT/TP links.

The VAN providers suggested that transactions be encrypted using PGP. This will allow confidentiality services between the VAN and the

TP.

One of the VANs providers stated that some DOD contractors have expressed concern with the TS 241s. Many trading partners have required that the VAN encrypt all data and expressed concern with the ECPN handling data. This particular VAN provider suggested that transactions be encrypted, wrapped in the BIN segment of a TS 841, and transmitted to the intended destination. The contents of the 841 cannot be verified and therefore reconciliation of the transaction is not available. The TS 841 solution does not provide a solution for public transactions.

It was suggested that security be implemented as a separate layer similar to that used for the communications functions.

It was suggested that a hybird security solution be proposed whereas digital signature is applied at the transaction level only and a secure socket layer provide encryption for the entire file. This is an interim solution that can be replaced with the target security solution. Group members felt that an interim solution would become permanent and therefore should not be considered. Postponing implementation of X12.58 until version 4010 is approved will have minimal impact on the legal community, but may have adverse effects on the medical, banking, and financial communities.

Some VANs expressed a desire to encrypt the entire transaction, including the ISA, rather than having security applied at the GS or TS level.

Part 10 is the only place to date where X12 security is addressed. It is a directive document and contractually enforceable. It was brought out that point-to-point security is not addressed in Part 10. The two links between AIS/ECPN and VAN/TP cannot receive X12 documents. It was suggested that this issue be addressed in section 10.5

It was suggested that a requirements matrix be developed. User's would implement security based on the connectivity and security service required. This approach is similar to the requirements matrix used by the District Court of New Mexico. See their web site at www.nmcourt.fed.us. This site describes how they are using EDI and digital signatures.

VANs and Gateways will undergo the same certification process.

It was suggested that two types of security be addressed in section 10.5: X12.58 in the future and a form of encryption and digital signature now. The ECPN will be a trusted agent that can re-sign and re-encrypt received data on behalf of the Government.

It was brought out that if the Government requires point-to-point security, for data encrypted at the file level, a VAN provider needs to know whether or not it is required to protect the data after leaving the VAN domain. While usually the Government cannot impose requirements outside its domain, they can enforce requirements to insure compliance with existing Federal laws.

There are no security products that apply the Digital Signature Standard to an interchange.

9. ISA/GS/Security Segment Updates. The group approved editorial and technical changes to the ISA and GS segments. The security segments were deleted. These changes were incorporated in the revised Part 10.

10. TS 242 IC changes. The group approved editorial and technical changes to the TS 242 IC. These changes were incorporated in the revised 3070 242 IC.

11. 997 Functional Acknowledgment changes. The group approved editorial and technical changes to the 997 Functional Acknowledgment. These changes were incorporated in the revised Part 10.

12. Action Items. The following action items were recorded at the April meeting:

Action Item: An e-mail will be sent out by the Chair to the CCSFWG membership requesting that the voting reps and alternates be identified.
Tasked to: Chair
Completed: 7 April 1997

Action Item: Provide electronic copy of the revised CCSFWG charter for comment.
Tasked to: Chair
Completed: 6 April 1997

Action Item: Staff security white paper electronically and related comments
Tasked to: Chair
Completed: 6 April 1997

Action Item: Add the following text in the VLA: Within an interchange, all GS02/GS03 code pairs shall be identical throughout the interchange. In the case of a public transaction, an additional limitation shall allow for only one transaction set per group, one group per interchange."
Tasked to: Will Griffith/Chair

Action Item: It was brought out that if the Government requires point-to-point security, for data encrypted at the file level, a VAN provider needs to know whether or not it is required to protect the data after leaving the VAN domain.
Tasked to: Chair

Action Item: Agenda for May Security Meeting
Tasked to: Chair

Action Item: Provide a strawman Requirements Matrix for the May Security Meeting
Tasked to: Dan Codman

Action Item: Provide copies of GAO Report
Tasked to: Linda Boerkoff/Chair

13. Closing Remarks. Mr. Curtis stated that open forum meetings should be held as often as issues that can be addressed in this forum arise. A meeting to discuss security issues is tentatively scheduled for 13-15 May 1997. Agenda items should include functional security requirements, X12.58, and security solutions. With no other business to discuss, Mr. Curtis adjourned the meeting at 1415 hours, on Wednesday, 2 April 1997.

(NOTE: For those who requested it, the "Truths" document is attached to this email in ASCII format.)

****
* Lebbeus "Lib" Curtis VII * Phone: (703) 735-3203, DSN: 653- *
* Chairman, Joint Federal/DOD * Fax: (703) 735-3194, DSN: 653- *
* Communications, Control & * INTERNET: curtisl@ncr.disa.mil *
* Security Functional WG * w/MIME edi@itsi.disa.mil *
* 10701 Parkridge Boulevard * curtisl@ncrm.disa.mil *
* Reston, Virginia 20191-4357 * lcurtis@edi.oti.disa.mil *
****

The following is an attached File item from cc:Mail. It contains information that had to be encoded to ensure successful transmission through various mail systems. To decode the file use the UUDECODE program.

---------- Cut Here ----------
begin 644 truths.txt
M07!P96YD:7@@02`M(%1R=71H<R`-"B`@("`@#0H@,2X@5&AE('1W;R!M;W-T
M(&-O;6UO;B!E;&5M96YT<R!I;B!T:&4@=6YI=F5R<V4@87)E(&AY9')O9V5N
M(&%N9"`-"B`@("`@<W1U<&ED:71Y+@T*("`@("`-"B`R+B!);F1E8VES:6]N
M(&ES('1H92!K97D@=&\@9FQE>&EB:6QI='DN#0H@("`@(`T*(#,N(%1H92!T
M<F]U8FQE('=I=&@@9&]I;F<@<V]M971H:6YG(')I9VAT('1H92!F:7)S="!T
M:6UE(&ES('1H870@;F]B;V1Y("`@("`@#0H@("`@(&%P<')E8VEA=&5S(&AO
M=R!D:69F:6-U;'0@:70@=V%S+@T*("`@("`-"B`T+B!4:&4@9F%C=',L(&%L
M=&AO=6=H(&EN=&5R97-T:6YG+"!A<F4@=7-U86QL>2!I<G)E;&5V86YT+@T*
M("`@("`-"B`U+B!$96IA($UO;SH@5&AE(&9E96QI;F<@=&AA="!Y;W4G=F4@
M:&5A<F0@=&AI<R!B=6QL(&)E9F]R92X-"B`@("`@#0H@-BX@4V]M92!D87D@
M;7D@<VAI<"!W:6QL(&-O;64@:6XL(&)U="!W:71H(&UY(&QU8VLL($DG;&P@
M8F4@870@=&AE(`T*("`@("!A:7)P;W)T+@T*#0H@-RX@270@;6%Y(&)E('1H
M870@>6]U<B!S;VQE('!U<G!O<V4@:6X@;&EF92!I<R!S:6UP;'D@=&\@<V5R
M=F4@87,@82`-"B`@("`@=V%R;FEN9R!T;R!O=&AE<G,N#0H@("`@(`T*(#@N
M($UO;F5Y(&-A;B=T(&)U>2!H87!P:6YE<W,N($)U="!I="!S=7)E(&UA:V5S
M(&UI<V5R>2!E87-I97(@=&\@;&EV92`@("`@#0H@("`@('=I=&@N#0H@("`@
M(`T*(#DN($%L=V%Y<R!R96UE;6)E<B!T;R!P:6QL86=E(&)E9F]R92!Y;W4@

M8G5R;BX-"B`@("`@#0HQ,"X@268@(F-L;W1H97,@;6%K971H('1H92!M86XB
M('1H96X@:70@9F]L;&]W<R!T:&%T(&YA:V5D('!E;W!L92!H879E(`T*("`@
M("!L:71T;&4@;W(@;F\@:6YF;'5E;F-E(&]N('-O8VEE='DN#0H@("`@("`-
M"C$Q+B!6:71A;"!P87!E<G,@=VEL;"!D96UO;G-T<F%T92!T:&5I<B!V:71A
M;&ET>2!B>2!M;W9I;F<@=&\@=VAE<F4@>6]U(`T*("`@("!C86XG="!F:6YD
M('1H96TN#0H-"C$R+B!4:&4@;&%W(&]F(%!R;V)A8FEL:71Y($1I<W!E<G-A
M;"!D96-R965S('1H870@=VAA=&5V97(@:70@:7,@=&AA="!H:71S(`T*("`@
M("!T:&4@9F%N('=I;&P@;F]T(&)E(&5V96YL>2!D:7-T<FEB=71E9"X@#0H@
M("`@(`T*,3,N($EF(&%T(&9I<G-T('EO=2!D;VXG="!S=6-C965D+"!S:WED
M:79I;F<@:7,@;F]T(&9O<B!Y;W4N#0H@("`@(`T*,30N(%1H97)E(&ES(&%B
M<V]L=71E;'D@;F\@<W5B<W1I='5T92!F;W(@82!G96YU:6YE(&QA8VL@;V8@
M<')E<&%R871I;VXN(`T*#0HQ-2X@2&%P<&EN97-S(&ES(&UE<F5L>2!T:&4@
M86)S96YC92!O9B!P86EN+@T*("`@("`-"C$V+B!.;W-T86QG:6$@:7-N)W0@
M=VAA="!I="!U<V5D('1O(&)E+@T*("`@("`-"C$W+B!0<WEC:&EA=')I<W1S
M('-A>2!T:&%T(&]N92!O=70@;V8@9F]U<B!P96]P;&4@87)E(&UE;G1A;&QY
M(&EL;"X@0VAE8VL@#0H@("`@('1H<F5E(&9R:65N9',N($EF('1H97DG<F4@
M3TLN+BX-"B`@("`@#0HQ."X@5&AE(&-A<F5F=6P@87!P;&EC871I;VX@;V8@
M=&5R<F]R(&ES(&%L<V\@82!F;W)M(&]F(&-O;6UU;FEC871I;VXN(`T*#0HQ
M.2X@5&AI;F=S(&%R92!M;W)E(&QI:V4@=&AE>2!A<F4@=&]D87D@=&AA;B!T
M:&5Y(&5V97(@:&%V92!B965N(&)E9F]R92X@#0H@("`@(`T*,C`N($5V97)Y
M=&AI;F<@<VAO=6QD(&)E(&UA9&4@87,@<VEM<&QE(&%S('!O<W-I8FQE+"!B
M=70@;F\@<VEM<&QE<BX-"@T*,C$N($9R:65N9',@;6%Y(&-O;64@86YD(&=O
M+"!B=70@96YE;6EE<R!A8V-U;75L871E+@T*("`@("`-"C(R+B!)9B!Y;W4@
M8V%N('-M:6QE('=H96X@=&AI;F=S(&=O('=R;VYG('1H96X@>6]U(&AA=F4@
M<V]M96]N92!I;B!M:6YD('1O(`T*("`@("!B;&%M92X-"B`@("`@#0HR-2X@
M3VYE+7-E=F5N=&@@;V8@;&EF92!I<R!S<&5N="!O;B!-;VYD87DN#0H@("`@
M(`T*,C8N($)Y('1H92!T:6UE('EO=2!C86X@;6%K92!E;F1S(&UE970L('1H
M97D@;6]V92!T:&4@96YD<RX-"B`@("`@#0HR-RX@3F]T(&]N92!S:')E9"!O
M9B!E=FED96YC92!S=7!P;W)T<R!T:&4@;F]T:6]N('1H870@;&EF92!I<R!S
M97)I;W5S+@T*#0H@,C@N(%1H:7,@:7,@87,@8F%D(&%S(&ET(&-A;B!G970@
M+6)U="!D;VXG="!B970@;VX@:70N#0H@("`@(`T*,CDN($YE=F5R('=R97-T
M;&4@=VET:"!A('!I9RX@66]U(&)O=&@@9V5T(&1I<G1Y(&)U="!O;FQY('1H
M92!P:6<@96YJ;WES(`T*("`@("!I="X-"B`@("`@#0HS,"X@5&AE('1R;W5B
M;&4@=VET:"!L:69E(&ES('1H870@>6]U(&%R92!H86QF=V%Y('1H<F]U9V@@
M:70@8F5F;W)E('EO=2`-"B`@("`@(')E86QI>F4@:70G<R!A(")D;R!I="!Y
M;W5R<V5L9B(@=&AI;F<N#0H@("`@(`T*,S$N($1R:6YK('9A<FYI<V@@86YD
M('EO=2=L;"!G970@82!L;W9E;'D@9FEN:7-H+@T*("`@("`-"C,R+B!792!C
M86X@<WEM<&%T:&EZ92!W:71H(&$@8VAI;&0@=VAO(&ES(&%F<F%I9"!O9B!T
M:&4@9&%R:RP@8G5T('1H92`-"B`@("`@('1R86=E9'D@;V8@;&EF92!I<R!T
M:&%T(&UO<W0@<&5O<&QE(&%R92!A9G)A:60@;V8@=&AE(&QI9VAT+@T*("`@
M("`-"C,S+B!)9B!O;FQY('1H92!G;V]D(&1I92!Y;W5N9R!T:&5N('=H870@
M9&]E<R!T:&%T('-A>2!A8F]U="!S96YI;W(@#0H@("`@("!C:71I>F5N<S\-
M"B`@("`@#0HS-"X@16UP;&]Y('1E96YA9V5R<R`M('=H:6QE('1H97D@:VYO
M=R!E=F5R>71H:6YG+B`-"B`@("`@#0HS-2X@5&AE(&)E<W0@86YT:7%U97,@
M87)E(&]L9"!F<FEE;F1S+@T*("`@("`-"C,V+B!$;W=N('=I=&@@9W)A=FET

```
M>2$-"B`@("`@#0HS-RX@3F]B;V1Y)W,@<&5R9F5C="!A;F0@<VEN8V4@22=M
M(&YO8F]D>2XN+B$@#0H@("`@(`T*,S@N(%=H>2!I<R!T:&5R92!O;FQY(&]N
M92!-;VYO<&]L:65S($-O;6UI<W-I;VX_#0H@("`@(`T*,SDN($ET(&AA<R!R
M96-E;G1L>2!B965N(&1I<V-O=F5R960@=&AA="!R97-E87)C:"!C875S97,@
M8V%N8V5R(&EN(')A=',N("`-"B`@("`@#0H-"C0P+B!!9V4@:7,@82!C87-E
M(&]F(&UI;F0@;W9E<B!M871T97(N($EF('EO=2!D;VXG="!M:6YD('1H96X@
M:70@<F5A;&QY("`@("`@#0H@("`@(&1O97-N)W0@;6%T=&5R+@T*("`@("`-
M"C0Q+B!7:&5N('1H92!C870G<R!A=V%Y('1H97)E(&%R92!F97=E<B!H86ER
M<R!O;B!T:&4@87)M8VAA:7(N#0H@("`@(`T*-#(N($%N(&5X<&5R="!I<R!N
M;W1H:6YG(&UO<F4@=&AA;B!A;B!O<F1I;F%R>2!P97)S;VX@87=A>2!F<F]M
M(&AO;64N(`T*("`@("`-"C0S+B!)9B!Y;W4@8V%N)W0@8F4@:VEN9"P@8F4@
*=F%G=64N#0H-"@``

end
```